NEMZETI KUTATÁSI, FEJLESZTÉSI ÉS INNOVÁCIÓS HIVATAL
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Kibernyomozói munka terepen

A Btk. XLIII. Fejezetében szabályozott tiltott adatszerzés és az információs rendszer elleni bűncselekmények kapcsán felmerülő egyes jogi minősítési és elhatárolási kérdésekről a joggyakorlat tükrében

I. Szabályozási háttér

Az információs rendszereket ért támadások tárgyában a jelenlegi magyar büntető anyagi jogi szabályozás alapját két nemzetközi dokumentum, az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezménye (a továbbiakban: Budapesti Egyezmény)[1], illetve az Európai Parlament és a Tanács információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról szóló 2013. augusztus 12-i 2013/40/EU irányelve (a továbbiakban: Irányelv) adja.

Magyarország Budapesti Egyezményhez történt csatlakozását követően a jogalkotó – az Egyezménnyel összhangban[2] – a Büntető Törvénykönyvről szóló 1978. évi IV. törvénybe (a továbbiakban: régi Btk.) 2002. április 1. napi hatállyal új bűncselekményeket iktatott be. A régi Btk. 'Gazdasági bűncselekmények' fejezete 'Gazdálkodási kötelességeket és a gazdálkodás rendjét sértő bűncselekmények' címében – felváltva a számítógépes csalás törvényi tényállását – került elhelyezésre a 300/C. §-ban szabályozott számítástechnikai rendszer és adatok elleni bűncselekmény, továbbá az új 300/E. §-ban a számítástechnikai rendszer védelmét biztosító technikai intézkedés kijátszása. Emellett módosításra került a régi Btk. 178/A. §-ában szabályozott magántitok jogosulatlan megismerése vétségének tényállása is oly módon, hogy a hírközlő berendezés útján, illetőleg számítástechnikai rendszeren másnak továbbított közlemény, illetve adat kifürkészését és technikai eszközzel történő rögzítését is büntetendővé nyilvánították.

[1] A Budapesti Egyezményt Magyarország 2001. november 23. napján írta alá, majd 2003. december 4. napján ratifikálta, azt a 2004. évi LXXIX. törvény hirdette ki, rendelkezéseit 2004. július 1. napjától kell alkalmazni.

[2] A Budapesti Egyezmény anyagi jogi szempontból négy bűncselekményi kategóriát különböztet meg: a számítástechnikai rendszer és számítástechnikai adat hozzáférhetősége, sértetlensége és titkossága elleni bűncselekmények (jogosulatlan belépés, jogosulatlan kifürkészés, számítástechnikai adat megsértése, számítástechnikai rendszer megsértése, eszközökkel való visszaélés), a számítógépekkel kapcsolatos bűncselekmények (számítógéppel kapcsolatos hamisítás, számítógéppel kapcsolatos csalás), a számítástechnikai adat tartalmával kapcsolatos bűncselekmények (gyermekpornográfiával kapcsolatos bűncselekmények), illetve a szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekmények. A Budapesti Egyezmény Első Kiegészítő Jegyzőkönyve az információs rendszer útján megvalósított rasszista és idegengyűlölő cselekmények büntetendővé nyilvánítása kapcsán fogalmaz meg előírásokat.

A TKP2021-NVA-18 számú projekt a Kulturális és Innovációs Minisztérium Nemzeti Kutatási, Fejlesztési és Innovációs Alapból nyújtott támogatásával, a TKP2021 pályázati program finanszírozásában valósult meg.

A régi Btk.-t felváltó, a Büntető Törvénykönyvről szóló 2012. évi C. törvény (a továbbiakban: Btk.) megalkotása során az információs rendszert érintő bűncselekmények szabályozására a Budapesti Egyezményen, valamint az Európa Tanács információs rendszerek elleni támadásokról szóló 2005/222/IB kerethatározatának (a továbbiakban: Kerethatározat) rendelkezésein alapulva külön fejezetben, a tiltott adatszerzés és az információs rendszer elleni bűncselekmények címet viselő XLIII. Fejezetben került sor. A törvényi tényállások újraszabályozása során lényegét tekintve a régi Btk. 300/C. §-ában szabályozott tényállást két külön bűncselekményre, a Btk. 423. §-a szerinti információs rendszer és adatok elleni bűncselekményre (régi Btk. 300/C. § (1)-(2) bekezdés) és a vagyon elleni bűncselekmények között szabályozott, a Btk. 375. § (1) bekezdésébe ütköző információs rendszer felhasználásával elkövetett csalás bűncselekményére (régi Btk. 300/C. § (3)-(4) bekezdés) bontották, míg a számítástechnikai rendszer védelmét biztosító technikai intézkedés kijátszása mint sui generis előkészületi bűncselekmény megnevezése módosítása mellett önálló tényállási keretét megtartva a Btk. 424. §-ában került szabályozásra. A Kerethatározat fogalomhasználata mentén az addig használt számítástechnikai rendszer kifejezést felváltotta az információs rendszer szóhasználat.

A miniszteri indokolás szerint a hatályos Btk. azért emelte ki a gazdálkodás rendjét sértő bűncselekmények köréből az információs rendszer elleni bűncselekményeket, mert ezek jogi tárgya nem a gazdálkodás rendjének megsértése, hanem az információs rendszer megfelelő működtetéséhez és az abban foglalt adatok megőrzéséhez fűződő társadalmi érdek védelme. Tekintettel arra, hogy a tiltott adatszerzés bűncselekmény egyik elkövetési fordulatát is számítástechnikai rendszer útján valósítják meg, mely magatartás ugyancsak a Budapesti Egyezmény megsértését jelenti, indokolttá vált e bűncselekményt az információs rendszer elleni bűncselekményekkel egy fejezetben kezelni.

Az új Btk. hatályba lépését követően a Kerethatározatot felváltotta az Irányelv[3], melynek való megfelelés érdekében 2015. január 1. napi hatállyal módosították az információs rendszer vagy adat megsértése tényállása szabályozásának felépítését, illetve az adatvisszaélés jellegű elkövetési magatartások büntetési tételét felemelték[4], emellett bővítették a Btk. 424. §-ában szabályozott információs rendszer védelmét biztosító technikai intézkedés kijátszása bűncselekmény tényállását a tiltott adatszerzés Btk. 422. § (1) bekezdés d) pontjában szabályozott elkövetési magatartási fordulatával. Az Irányelvnek való maradéktalan megfelelés érdekében továbbá 2023. január 1. napi hatállyal az információs rendszer vagy adat megsértése minősített eseteinek körét bővítették a jelentős érdeksérelem okozásával.

---

[3] Az Irányelv 3-6. Cikkei az információs rendszerek elleni támadások körében az információs rendszerekhez való jogellenes hozzáférés, a rendszert, valamint az adatot érintő jogellenes beavatkozás és a jogellenes adatszerzés vonatkozásában állapítanak meg minimumszabályokat.

[4] A büntetések, az intézkedések, egyes kényszerintézkedések és a szabálysértési elzárás végrehajtásáról szóló 2013. évi CCXL. törvény és ehhez kapcsolódóan más törvények módosításáról szóló 2014. évi LXXII. törvény indokolása e körben rögzíti, hogy az Irányelv 9. cikk (4) bekezdése az információs rendszert vagy adatot érintő jogellenes beavatkozás bűncselekmények – amelyek az akkor hatályos Btk. 423. § (1) bekezdés b) és c) pontjaiban szabályozott bűncselekményeket fedték le – bűnszervezetben történő elkövetése esetére legalább öt évig terjedő szabadságvesztés büntetést határoz meg. A Btk. az említett bűncselekményeket a módosítást megelőzően csak két évig terjedő szabadságvesztéssel rendelte büntetni, így amennyiben e bűncselekmények elkövetésére bűnszervezetben került volna sor, a Btk. 91. §-ában megállapított, a bűnszervezetben történő elkövetésre vonatkozó rendelkezések alapján is – figyelemmel arra, hogy ilyen esetben a büntetési tétel felső határa kétszeresére emelkedik – csak négy évig terjedő szabadságvesztést lehetett volna kiszabni. Erre tekintettel indokolt volt a két bűncselekmény esetén a büntetési tétel felemelése három évig terjedő szabadságvesztésre.

II. A tiltott adatszerzés

1. A tiltott adatszerzés *első alapesetét* a Btk. 422. § (1) bekezdése szabályozza, ez az elkövetési magatartás alapján öt részesetre bontható le. A tiltott adatszerzés első alapesetét követi el, aki személyes adat, magántitok, gazdasági titok vagy üzleti titok jogosulatlan megismerése céljából:
a) más lakását, ahhoz tartozó egyéb helyiségét vagy az azokhoz tartozó bekerített helyet titokban átkutatja,
b) más lakásában, ahhoz tartozó egyéb helyiségében vagy az azokhoz tartozó bekerített helyen történteket technikai eszköz alkalmazásával titokban megfigyeli vagy rögzíti,
c) más postai küldeményét vagy egyéb zárt küldeményét titokban felbontja vagy megszerzi, és annak tartalmát technikai eszközzel rögzíti,
d) elektronikus hírközlő hálózat vagy eszköz útján, illetve információs rendszeren folytatott kommunikáció tartalmát titokban kifürkészi, és az észlelteket technikai eszközzel rögzíti,
e) információs rendszerben kezelt adatokat titokban kifürkész, és az észlelteket technikai eszközzel rögzíti.

i. A bűncselekmény elkövetésének módja a titokban történő átkutatás, megfigyelés, rögzítés, felbontás, megszerzés és kifürkészés. Ez minimálisan feltételezi azt, hogy az elkövetőnek arra kell törekednie, hogy cselekményét a passzív alany ne észlelje. Amennyiben tehát ezen elkövetési magatartások végrehajtására a passzív alany jelenlétében, illetve tudtával kerül sor – függetlenül attól, hogy ellene tiltakozik – úgy a tiltott adatszerzés bűncselekmény megállapítására nincs lehetőség.[5]

ii. A védett jogi tárgy – a személyes adat, magántitok, gazdasági titok vagy üzleti titok védelméhez fűződő érdek – eltérő voltára figyelemmel a tényállás a) és b) pontjaiban szabályozott fordulatai halmazatban állhatnak a házi jogot védelmező magánlaksértés bűncselekményével abban az esetben, ha mindkét védett jogi tárgy sérül. Ha az elkövető azonban egyébként jogszerűen tartózkodik a passzív alany lakásában és e közben hajtja végre a sértett tudta nélkül a titkos kutatást vagy helyezi el a későbbi titkos megfigyeléshez szükséges technikai eszközt, úgy a két cselekmény halmazata nem lesz megállapítható.

iii. A BH2014. 263. analógiájára nem követi el a tiltott adatszerzés bűntettének Btk. 422. § (1) bekezdésének b) pontjában szabályozott fordulatát az, aki más lakásában titokban fényképfelvételeket készít, de a lakással rendelkező engedélyével, tudtával tartózkodik a lakásban. A magántitok jogosulatlan megismerésének bűntette miatt folyamatban volt kapcsolódó ügyben ugyanis a Kúria kimondta, hogy figyelemmel arra, hogy a terhelt jogszerűen tartózkodott a sértett lakásában, jogosult volt annak vizuális képe megismerésére, ekként a lakásban fényképek készítésével magántitok jogosulatlan megismerése nem lehetett a célja, ez pedig a bűncselekmény megállapítását már önmagában is kizárja. Hasonlóan – a BH2014. 134. analógiájára – nem követi el a tiltott adatszerzés bűntettét az, aki a vele folytatott beszélgetés tartalmát titokban rögzíti, még akkor sem, ha erre más magánlakásában kerül sor. A kapcsolódó, szintén magántitok jogosulatlan megismerésének bűntette miatt indult ügyben ugyanis a Kúria kimondta, hogy a sértett által a

[5] Azonban pl. jogszerű hatósági kutatás végrehajtásának színlelése esetén a magánlaksértés megállapíthatósága vizsgálandó.

terhelttel önként közölt adatok rögzítése nem tekinthető kifürkészésnek, függetlenül attól, hogy a felvétel készítéséről a sértettnek nem volt tudomása.

iv. Az első alapeset c-e) pontjaiban szabályozott fordulatok elkövetési módja a titokban történő felbontás, megszerzés, illetve kifürkészés végrehajtása, mely cselekmények célja az érintett küldemény, kommunikáció, illetve adat tartalmának technikai eszközzel történő rögzítése. Minderre figyelemmel, technikai eszközzel történő rögzítési cél hiányában a cselekmény a Btk. 224. §-ában szabályozott levéltitok megsértése bűncselekmény[6] megállapítására lehet alkalmas.

2. A bűncselekmény Btk. 422. § (1a) bekezdésében szabályozott *második alapesetét* követi el, aki személyes adat, magántitok, gazdasági titok vagy üzleti titok jogosulatlan megismerése céljából
a) nyilvános vagy a közönség részére nyitva álló helyen kívül más helyiséget vagy területet, – a közösségi közlekedési eszköz kivételével – járművet, továbbá más használatában levő tárgyat titokban átkutat,
b) nyilvános vagy a közönség részére nyitva álló helyen kívül más helyiségben vagy területen, továbbá – a közösségi közlekedési eszköz kivételével – járművön történteket titokban technikai eszköz alkalmazásával megfigyeli vagy rögzíti.

i. Az elkövetési magatartások egyeznek az első alapeset a) és b) pontjaiban szabályozott fordulataival, azonban a bűncselekmény elkövetésére más helyszíneken kerülhet sor.

A 2018. január 1. napja óta hatályos második alapeseti szabályozás előzményeként szükséges felhívni a Kúria Bfv.III.299/2017. számú ügyben hozott döntését, mely szerint a tiltott adatszerzés bűntettét nem valósítja meg, aki mozgásérzékelős, felvételek készítésére alkalmas kamerát munkahelyén, a kft. női mosdójában szerel fel az ott történtek rögzítése céljával. A Kúria indokolása szerint a bűncselekmény ilyen természetű elkövetési magatartása az ekkor hatályos törvényi szabályozás, vagyis az (1) bekezdés a) és b) pontjainak rendelkezései alapján csak más (magán)lakásában, egyéb helyiségében, vagy azokhoz tartozó bekerített helyen valósítható meg, munkahelyen, hivatali helyiségben, munkahely közös használatú helyiségeiben nem. Az elkövetés helyszíne a bűncselekmény különös részi törvényi tényállásának szükségszerű, nélkülözhetetlen eleme. A Kúria döntését követően módosították a tiltott adatszerzés bűntettének tényállását oly módon, hogy azt kiegészítették az (1a) bekezdéssel, mely bővítette azon helyek listáját, ahol a bűncselekmény bizonyos elkövetési magatartásainak megvalósítása szankcionálhatóvá vált.

ii. A törvényi tényálláshoz fűzött miniszteri indokolás – utalva a Kúria Bfv.III.299/2017. számú ügyben hozott döntésére – kifejti, hogy e bekezdés törvénybe iktatására azért került sor, hogy minden olyan magatartás szankcionálható legyen, amely során a magánszemély elkövető alapvetően zárt térben olyan titkosszolgálati/leplezett eszközt alkalmaz, amelyhez – ha azt hatóság végezné – a hatóságnak bírói engedélyre lenne szüksége. Az ilyen helyen tartózkodók ugyanis joggal számítanak bizonyos fokú védettségre személyes adataikat, magántitkaikat, gazdasági, illetve üzleti titkaikat illetően. Annak érdekében, hogy a jogalkotói szándék maradéktalanul érvényesüljön és a jogértelmezési probléma megoldódjon, a törvény a tiltott adatszerzés

[6] A Btk. 224. §-ának (1) bekezdése szerint, aki a) másnak közlést tartalmazó zárt küldeményét megsemmisíti, a tartalmának megismerése végett felbontja, megszerzi, vagy ilyen célból illetéktelen személynek átadja, illetve b) elektronikus hírközlő hálózat – ideértve az információs rendszert is – útján másnak továbbított közleményt kifürkész, ha súlyosabb bűncselekmény nem valósul meg, vétség miatt elzárással büntetendő. Súlyosabban minősül a bűncselekmény, ha azt foglalkozás vagy közmegbízatás felhasználásával követik el, továbbá akkor, ha az jelentős érdeksérelmet okoz.

bűncselekmény elkövetési helyét tágabban határozza meg, oly módon, hogy a bárki számára hozzáférhető helyen vagy a közösségi közlekedési eszközökön történt tiltott adatszerzés továbbra sem lesz szankcionálható.

iii. A tiltott adatszerzés Btk. 422. § (1a) bekezdésének b) pontjába ütköznek tipikusan azon cselekmények, melyek során az elkövető alapvetően szűkebb közönség részére nyitva álló intézmény irodájában, zuhanyzójában, mosdójában vagy próbafülkéjében tartózkodó személyekről készít fénykép, illetve videófelvételt. Az egyik ilyen jellegű ügyben[7] megállapítható tényállás lényege szerint a férfi elkövető egy bevásárlóközpont női mosdójának fülkéjébe bement, majd a telefonját a térelválasztó fal alatt átnyújtva a szomszédos fülkében vizeletét ürítő személyről fényképfelvételeket készített. A képeken a sértett nemi szerve takarásban volt, azokon fedetlenül kizárólag combja volt látható. Az elkövető a képeket nem használta fel, azokat a mobiltelefonjáról törölte, a képek visszaállítására szakértő bevonásával került sor. Az ügyben az elkövető gyanúsítotti kihallgatására a Btk. 205. § (3) bekezdésébe ütköző szeméremsértés vétsége[8] miatt került sor, a megállapított tényállás kapcsán azonban szükséges volt vizsgálni a tiltott adatszerzés Btk. 422. § (1a) bekezdésének b) pontjába ütköző fordulatának megállapíthatóságát, ezen belül pedig elsődlegesen azt, hogy a bevásárlóközpont nyilvános mosdójának WC fülkéje a törvényi tényállás által megkövetelt kritériumoknak megfelelő elkövetési hely-e.

A miniszteri indokolást alapul véve az elkövetési hely vonatkozásában az elhatárolás alapját az adja, hogy adott helyen a leplezett eszköz alkalmazásához a hatóságnak bírói engedélyre lenne-e szüksége. E körben két leplezett eszköz, a bírói engedélyhez nem kötött rejtett figyelés[9] és a bírói engedélyhez kötött titkos megfigyelés[10] vizsgálata szükséges. A rejtett figyelés mindig külső megfigyelést jelent: melyik lakásból lépett ki az érintett személy, milyen útvonalon haladt, kikkel találkozott, mit cselekedett a nyilvános vagy közönség számára nyitva álló területeken, milyen tárgyakat viselt vagy mit vitt magával.[11] A bírói engedélyhez kötött leplezett eszközök mélyebben hatolnak a magánéletbe, érintik a lakás, egyéb helyiség, bekerített hely, jármű, megfigyelt tárgy belsejét.[12] A hely titkos megfigyelése kapcsán rögzíthető, hogy – a magánlaksértés, illetve tiltott adatszerzés lakás fogalmához képest – szélesebb körben használja a lakás fogalmát, benne foglaltatik minden emberi tartózkodásra szolgáló, négy fallal és tetővel ellátott építmény; ami lehet

[7] A Fővárosi Főügyészségen G.3442/2022. számon iktatott bűnügy.

[8] Ha súlyosabb bűncselekmény nem valósul meg, a Btk. 205. § (3) bekezdésébe ütköző szeméremsértés vétségét követi el, aki mással szemben olyan szeméremsértő magatartást tanúsít, amely a sértett emberi méltóságát sérti.

[9] A Be. 215. § (5) bekezdése szerint a leplezett eszközök alkalmazására feljogosított szerv a bűncselekménnyel kapcsolatba hozható a) személyt, lakást, egyéb helyiséget, bekerített helyet, nyilvános vagy a közönség részére nyitva álló helyet, illetve járművet, vagy b) tárgyi bizonyítási eszközt képező dolgot titokban megfigyelhet, a történtekről információt gyűjthet, valamint az észlelteket technikai eszközzel rögzítheti. A törvényhely miniszteri indokolása szerint a rejtett figyelésnek a magánélet egyes színtereit, így például a magánlakást érintő alkalmazása a 232. §-ban meghatározott, hely titkos megfigyeléseként nevesített leplezett eszköz bírói engedélyhez kötött alkalmazásának szabályaira figyelemmel történhet.

[10] A Be. 232. § (3) bekezdése szerint a hely titkos megfigyelése során a leplezett eszközök alkalmazására feljogosított szerv bírói engedéllyel – a nyilvános vagy a közönség részére nyitva álló hely kivételével – a lakásban, egyéb helyiségben, bekerített helyen, illetve – a közösségi közlekedési eszköz kivételével – járművön történteket titokban technikai eszközzel megfigyelheti és rögzítheti. A törvényhely miniszteri indokolása alapján egyértelmű, hogy a megfigyeléshez használt technikai berendezés helyétől függetlenül a hely titkos megfigyelésének tárgya a felsorolt helyiségeken, helyeken belül történtek.

[11] Kommentár a büntetőeljárási törvényhez (főszerk.: Polt Péter), Wolters Kluwer Hungary Kft., 2018., 486. o.

[12] Kommentár a büntetőeljárási törvényhez (főszerk.: Polt Péter), Wolters Kluwer Hungary Kft., 2018., 486. o.

magánlakás, üdülő, iroda stb., így az egyéb helyiség és bekerített hely sem kizárólag lakáscélú helyiséghez kapcsolódik.[13]

Mindezt összevetve a tényállás bővítése, a tiltott adatszerzés bűntettének az (1a) bekezdésben meghatározott elkövetési magatartásokkal való kiegészítése mögött rejlő jogalkotói szándékkal – vagyis azzal, hogy a tényállás bővítésének célja az volt, hogy minden olyan magatartás szankcionálható legyen, amelyet az elkövető alapvetően zárt térben követ el –, arra vonható következtetés, hogy a nyilvános vagy a közönség részére nyitva álló helyen a vizsgált cselekmény elkövetésének ideje alatt is bárki számára hozzáférhető, kívülről is megfigyelhető helyet kell érteni. A közönség részére nyitva álló bevásárlóközpontban bárki által látogatható helyiségben lévő mosdófülke annak ajtaja becsukásával, bezárásával már nem minősül bárki számára hozzáférhető helynek, a fülkében tartózkodó személy joggal számíthat arra, hogy a fülkében tartózkodásának ideje alatt megilleti a személyes adatainak, így képmásának védelme, ekkor képmása megszerzése céljából róla engedélye nélkül fényképfelvétel nem készül. Minderre tekintettel az ilyen jellegű cselekmény nem a szubszidiárius szeméremsértés vétsége, hanem tiltott adatszerzés bűntette megállapítására alkalmas.

3. A bűncselekmény Btk. 422. § (2) bekezdésében szabályozott *harmadik alapesetét* követi el, aki fedett nyomozó, illetve titkos információgyűjtés folytatására vagy leplezett eszközök alkalmazására feljogosított szervvel titkosan együttműködő személy kilétének vagy tevékenységének megállapítása céljából az (1) bekezdésben meghatározottakon kívül információt gyűjt.

i. Amennyiben a törvényi tényállás e fordulatát jogosulatlan tevékenységével hivatalos személy követi el, úgy cselekménye a Btk. 307. §-ában[14] szabályozott jogosulatlan titkos információgyűjtés vagy leplezett eszköz jogosulatlan alkalmazása bűncselekmény megállapítására lehet alkalmas.[15]

***

A bűncselekmény első három alapesete célzatos bűncselekmény, az első két alapeset elkövetése során az elkövető cselekményét személyes adat, magántitok, gazdasági titok vagy üzleti titok jogosulatlan megismerése céljából, míg a harmadik alapeset véghezvitele során titkosan együttműködő személy kilétének vagy tevékenységének megállapítása végett követi el.

A célzat megállapításának fontosságára emlékeztet a Kúria Bfv.1548/2014/7. számú ügyben hozott ítélete. Az ügyben irányadó tényállás lényege szerint a terhelt a volt házastársával közösen használt családi házban lévő vonalas telefonra digitális hangfelvevőt szerelt, majd házastársa tudomása és beleegyezése nélkül beszélgetéseiről felvételeket készített, melyeket a felek között folyamatban

[13] Kommentár a büntetőeljárási törvényhez (főszerk.: Polt Péter), Wolters Kluwer Hungary Kft., 2018., 518-519. o.

[14] A Btk. 307. § (1) bekezdése szerint az a hivatalos személy, aki a) bíró vagy az igazságügyért felelős miniszter engedélyéhez kötött titkos információgyűjtést engedély nélkül végez, illetve bírói engedélyhez kötött leplezett eszközt engedély nélkül alkalmaz vagy az ezekre vonatkozó engedély kereteit túllépi, b) bíró vagy az igazságügyért felelős miniszter engedélyéhez kötött titkos információgyűjtést, illetve bírói engedélyhez kötött leplezett eszköz alkalmazását jogosulatlanul elrendeli vagy engedélyezi, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő. A (2) bekezdés szerint az (1) bekezdés szerint büntetendő az a hivatalos személy, akinek valótlan tényállítása alapján a bíró vagy az igazságügyért felelős miniszter engedélyéhez kötött titkos információgyűjtést, illetve a bírói engedélyhez kötött leplezett eszköz alkalmazását elrendelik vagy engedélyezik. A (3) bekezdés szerint a büntetés egy évtől öt évig terjedő szabadságvesztés, ha az (1)-(2) bekezdésben meghatározott bűncselekmény jelentős érdeksérelmet okoz.

[15] Büntetőjog II. Különös Rész (szerk.: Belovics Ervin), HVG-ORAC Lap- és Könyvkiadó, 2021., 541. o.

lévő házassági bontóperben benyújtott. A Kúria a terheltet az ellene tiltott adatszerzés bűntette miatt emelt vád alól felmentette. Az ítélet indokolása szerint megállapítható, hogy a terhelt szándéka (célja) a válófélben lévő felesége telefonbeszélgetéseinek lehallgatása, rögzítése, ezáltal megismerése, és a polgári perben bizonyítási eszközként történő felhasználása volt. Ugyanakkor a Btk. 422. § (1) bekezdése szerint a cselekmény akkor tényállásszerű, ha az elkövető célzata szűkebb, a tárgybeli ügyben kifejezetten a magántitok, mint a bűncselekmény egyik védett jogi tárgyának jogosulatlan megismerésére irányul, azonban a korábban eljárt bíróságok által az ügyben megállapított tényállás ilyen megállapítást nem tartalmaz. A Kúria álláspontja szerint kétségtelenül helytálló a másodfokú bíróság azon megállapítása, amely szerint „a sértett által másokkal folytatott telefonbeszélgetések rögzítése alkalmas volt arra, hogy a vádlott a sértett és más személyek magántitkai birtokába is juthasson". Ez a megállapítás azonban azt jelenti, hogy a telefonbeszélgetések rögzítése során esetlegesen magántitkok – gazdasági vagy üzleti titkok – is megismerhetők és rögzíthetők, ám ennek lehetőségéből mindössze a terhelt eshetőleges szándékára lehet következtetni, amely célzatos bűncselekmény esetében a bűnösség megállapításához nem elegendő.

Minderre tekintettel az ilyen jellegű cselekmények kapcsán indult bűnügyekben kiemelt jelentőséget kell tulajdonítani a nyomozás során annak, hogy a vizsgált elkövetési magatartás kapcsán a törvény által megkívánt célzat megállapítható-e, vagyis, hogy a bűncselekmény adott elkövetési magatartási fordulatának tanúsítására milyen célból, tehát személyes adat, magántitok, gazdasági titok vagy üzleti titok jogosulatlan megismerése, avagy titkosan együttműködő személy kilétének vagy tevékenységének megállapítása végett került-e sor.

Megjegyzést érdemel, az első alapeset c-e) pontjaiban szabályozott elkövetési magatartás kifejtése a speciális körbe tartozó titok megismerésére irányuló célzat megállapíthatóságának hiányában is alkalmas lehet – hasonlóan a technikai eszközzel történő rögzítés hiánya kapcsán már említett esethez – a Btk. 224. § (1) bekezdésében szabályozott levéltitok megsértése bűncselekmény megállapítására, mely kapcsán elegendő pusztán a jogellenes megismerési célzat bizonyítása.

***

4. A bűncselekmény Btk. 422. § (3) bekezdésében szabályozott *negyedik alapesetét* követi el, aki az (1)-(2) bekezdésben meghatározott módon megismert személyes adatot, magántitkot, gazdasági titkot vagy üzleti titkot továbbít vagy felhasznál.

i. A Kúria Bfv.162/2018/7. számú végzésének alapjául szolgáló ügyben irányadó tényállás lényege szerint ismeretlen személy megszerezte a terhelt volt élettársa, a sértett magánleveleit, melyeket a terheltnek átadott. A terhelt a sértettnek a gyermekelhelyezési perrel kapcsolatban az ügyvédjével folytatott levelezését, a nővérével váltott leveleit, ismerősének írt levelét és a barátnőjének írt levelét fellebbezése mellékleteként a folyamatban lévő polgári peres eljárásban a bírósághoz benyújtotta. A bíróság az ügyben a Btk. 422. § (3) bekezdésébe ütköző és az (1) bekezdése szerint büntetendő tiltott adatszerzés bűntettében mondta ki bűnösek a terheltet.

Végzésében a Kúria rögzítette, hogy a tiltott adatszerzés harmadik alapesete egyenes és eshetőleges szándékkal is megvalósítható, azonban a felhasználói tudatnak ki kell terjednie arra, hogy a kérdéses adatok (személyes adat, magántitok, gazdasági titok, üzleti titok) milyen módon lettek megszerezve, megismerve. A Kúria az ügyben – a védő érvelésével szemben – megállapította, hogy a terhelt tudatának ki kellett terjednie arra, hogy a felhasznált levelezés megszerzésére

jogellenes módon került sor. A bíróság indokolása szerint a körülményekre figyelemmel – a terhelt harmadik személytől a vele perben álló, ellenérdekű sértett négy különböző személlyel is folytatott, jelszóval védett, mégis a fiókjából kinyomtatott magánlevelezését vette át, melynek a terhelt sem feladója, sem címzettje nem volt, a magánlevelezés pedig a tartalmát tekintve alkalmasnak mutatkozott az ellentétes perbeli oldalon álló terhelt pozíciójának erősítésére – nincs észszerű alapja és ennélfogva indoka sem annak a következtetésnek, hogy a terhelt tudattartalma a nyilvánvaló magántitkot tartalmazó levelezés átvételekor és felhasználásakor nem fogta át az ismeretlen személy elkövetői magatartását.

***

A tiltott adatszerzés első négy alapesetének minősített esetei a hivatalos eljárás színlelésével, az üzletszerűen, a bűnszövetségben, valamint a jelentős érdeksérelmet okozva történő elkövetés.

***

5. Ha más bűncselekmény nem valósul meg, a bűncselekmény Btk. 422/A. § (1) bekezdésében szabályozott *ötödik alapesetét* követi el, aki pilóta nélküli légi jármű jogosulatlan használatával más lakását, egyéb helyiségét, vagy ezekhez tartozó bekerített helyet megfigyeli és az ott történteket rögzíti. A törvényhely (2) bekezdése szerint, ha más bűncselekmény nem valósul meg, szintén a tiltott adatszerzés bűntettét követi el, aki az (1) bekezdésben meghatározott megfigyelés során készített hang- vagy képfelvételt a nagy nyilvánosság számára hozzáférhetővé teszi.

i. A szubszidiárius ötödik alapeset első fordulatának elkövetési magatartása a rögzítéssel egyidejű megfigyelés. A titokban történő megfigyelés továbbra is a Btk. 422. §-a alapján büntetendő, ennek megfelelően az ötödik alapeset elkövetése miatt az a személy vonható felelősségre, aki az erre vonatkozó jogosultság nélkül a pilóta nélküli légi járművel történő nyílt (tehát az érintett személy által észlelhető módon való) megfigyelést végez.

ii. A szabálysértésekről, a szabálysértési eljárásról és a szabálysértési nyilvántartási rendszerről szóló 2012. évi II. törvény 166. § (1a) bekezdésébe ütköző magánlaksértés szabálysértésének megállapítására lehet alkalmas annak a személynek a cselekménye, aki a pilóta nélküli légi jármű jogosulatlan használata során más lakásáról, egyéb helyiségéről, vagy ezekhez tartozó bekerített helyről jogosulatlanul hang- vagy képfelvételt készít. A szabálysértési tényállás alá vonható tehát az az eset, amikor a megfigyelés – huzamosabb ideig történő figyelemmel kísérés – nem állapítható meg.[16]

iii. Ahogy arra a törvény miniszteri indokolása is felhívja a figyelmet, ha a pilóta nélküli légi járművel rögzített személyes adat jogosulatlan vagy céltól eltérő kezelése (így pl. drónnal felvétel készítése, akár repülési engedéllyel rendelkezik az elkövető, akár nem, akár lakott területen követik el, akár nem, akár egyszeri, egyedi képfelvétel készül, akár tartós megfigyelés történt) jelentős érdeksérelmet okoz, az továbbra is személyes adattal visszaélésként büntetendő.[17]

---

[16] Büntetőjog II. Különös Rész (szerk. : Belovics Ervin), HVG-ORAC Lap- és Könyvkiadó, 2021., 1001. o.

[17] A Btk. 219. § (1) bekezdése szerint, aki a személyes adatok védelméről vagy kezeléséről szóló törvényi vagy az Európai Unió kötelező jogi aktusában meghatározott rendelkezések megszegésével haszonszerzési célból vagy jelentős érdeksérelmet okozva a) jogosulatlanul vagy a céltól eltérően személyes adatot kezel, vagy b) az adatok biztonságát szolgáló intézkedést elmulasztja, vétség miatt egy évig terjedő szabadságvesztéssel büntetendő. Súlyosabban minősül

III. Az információs rendszer vagy adat megsértése

1. Az információs rendszer vagy adat megsértésének Btk. 423. § (1) bekezdésében szabályozott *első alapesetét* követi el, aki információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve vagy azt megsértve bent marad.

i. Az első alapeset első elkövetési fordulata, az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával történő jogosulatlanul belépés objektíve akkor valósulhat meg, ha az adott rendszer eleve védett a jogosulatlan használattól, felhasználói azonosító és jelszó, ujjlenyomat stb. alkalmazásával.[18] A védelmi intézkedés megsértésének minősül bármely olyan magatartás, amely nem a rendeltetésszerű hozzáférés útján teremti meg az elkövető hozzáférési lehetőségét az adathoz vagy a rendszer funkcióihoz.[19] Jellemző példája a jogosult jogosulatlan módon megszerzett jelszavának használata vagy annak kódtörő programmal való feltörése.

ii. A jogosultság kereteinek túllépése, illetve megsértése elkövetési magatartások vonatkozásában a Kúria a Bhar.537/2017/5. számú ítéletében rögzítette, hogy az ilyen jellegű cselekmény akkor minősül bűncselekménynek, ha az egyben a rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával – pl. más jelszavának a felhasználásával – történik; pusztán a jogosultság kereteinek túllépése nem éri el azt a veszélyességi szintet, mint amit az első fordulat megkíván. Mindezek alapján tehát ezen elkövetési magatartások gyakorlatban történő megállapítása csupán szűk elméleti lehetőségre szorítható, ugyanis a rendszer védelmét biztosító technikai intézkedés elsősorban az információs rendszer funkcióihoz történő hozzáférés viszonylatában értelmezhető és a jogosulatlan belépés megállapítása mellett a jogosulatlan bent maradás megállapításának a minősítés szempontjából már nincs jelentősége.[20] Felmerülhet ez alapján, hogy az elkövetés tényállásszerű megállapíthatóságához az információs rendszer olyan védelmére van szükség, amely a jogszerű hozzáférés valamilyen korlátozására is kiterjed, azonban az ilyen korlátozás megsértése jellemzően adatmanipulációval jár, így ebben az esetben a cselekmény már a tényállás (2) bekezdése szerint minősül.[21]

A gyakorlatban felmerült ügyben[22] megállapítható tényállás lényege szerint egy távközlési cég alkalmazottja munkaköri kötelezettségéből adódóan jogosult volt a cég géptermeiben az internet használatára. Az alkalmazott e jogosultságával visszaélt és az egyes telephelyek áramellátását használva bitcoin bányászatot végző informatikai eszközöket telepített a géptermekben, melyek számára az internetelérést a munkáltatója internetes hálózatára történő kapcsolódással biztosította. Az ügyben a gyanúsított kihallgatására az áramvételezéssel kapcsolatban a tíz millió forintot

---

a cselekmény, ha a személyes adattal visszaélést különleges adatra vagy bűnügyi személyes adatra, illetve hivatalos személyként vagy közmegbízatás felhasználásával követik el.

[18] Juhász Zsuzsanna et al.: Kommentár a Büntető Törvénykönyvről szóló 1978. évi IV. törvényhez, a Btk. 300/C. §-ához fűzött magyarázat (Jogtár Online)

[19] Szathmáry Zoltán: Hacking - Az információs rendszer és adat elleni bűncselekmény értelmezése, Infokommunikáció és Jog, 2022/2. szám, 9. o.

[20] Szathmáry i.m., 9. o.

[21] Szathmáry i.m., 9. o.

[22] A Fővárosi Főügyészségen G.2824/2020. számon iktatott bűnügy.

meghaladó elkövetési értékre figyelemmel lopás bűntette, míg az eszközök jogosulatlan telepítése okán információs rendszer vagy adat megsértésének vétsége miatt került sor. Az információs rendszer vagy adat megsértésének vétsége tekintetében azonban az volt megállapítható, hogy az információs rendszerbe történő belépés nem volt jogosulatlan, e körben technikai intézkedés megsértésére sem került sor, az alkalmazott munkakörénél fogva jogosult volt az internet használatára, a Kúria ítéletében foglaltak alapján pedig önmagában a szükséges mértéket, illetve időkorlátot megsértő rendszerben maradás nem bűncselekmény.

iii. Az információs rendszer vagy adat megsértésének vétsége eszközcselekménye lehet a Btk. 422. § (1) bekezdésének d) és e) pontjaiba ütköző tiltott adatszerzés bűntettének, mely esetben kizárólag utóbbi bűncselekmény megállapítására kerülhet sor.

2. Az információs rendszer vagy adat megsértésének Btk. 423. § (2) bekezdésének a) pontjában szabályozott *második alapesetét* követi el, aki az információs rendszer működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza.

i. A törvény az információs rendszerbe való jogosulatlan adatbevitelt önmagában nem tekinti szankcionálandó magatartásnak, csak akkor, ha az további, nem kívánt következményekhez vezet, így ha a rendszer működését akadályozza. Ennek oka a törvény miniszteri indokolása szerint a Budapesti Egyezménynek való megfelelés, mert a számítástechnikai adatok megsértésénél sem a Budapesti Egyezmény[23], sem a Kerethatározat – illetve a törvényi indokolást követően hatályba lépett Irányelv[24] – nem nevesíti a következményekkel nem járó adatbevitelt. Ezzel összefüggésben a Kúria – egyebek mellett – számítástechnikai rendszer és adatok elleni bűncselekményt is érintő EBH2009.2033. számú döntése mentén rögzíthető, hogy az információs rendszer működésének akadályozása magában foglalja azt az esetet is, amikor a rendszerbe valótlan adatok kerülnek be, és a további működése ezeken a valótlan adatokon alapul, ekként a rendszerben lévő adatok megbízhatóságához, hitelességéhez és titokban maradásához fűződő érdek sérül. Tehát akadályozáson nem csupán azt értjük, ha a rendszer teljesen leáll vagy annak működése akadozik, hanem azt is, ha a rendszer nem alkalmas a rendeltetésének megfelelő feladat ellátására.[25]

ii. A bíróság az információs rendszer vagy adat megsértése e fordulatában mondta ki bűnösnek azt a terheltet, aki a tehergépkocsi vezetőfülkéjének bal oldali ajtajába egy kapcsolót, a menetíró készülék érzékelőjébe és a jármű vezetőfülkéjébe egy-egy panelt szereltetett, amelynek segítségével a tehergépkocsi – menetidőt és sebességet is mérő – menetíró készülékét manipulálni tudta.[26]

---

[23] A Budapesti Egyezmény számítástechnikai rendszer megsértéséről szóló 5. cikke szerint: Minden Szerződő Fél megteszi azon jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy belső jogával összhangban bűncselekménynek minősüljön a számítástechnikai rendszer működésének számítástechnikai adatok bevitelével, továbbításával, megkárosításával, törlésével, megrongálásával, megváltoztatásával vagy megsemmisítésével való, jogosulatlan és szándékos, *jelentős mértékű akadályozása*.

[24] Az Irányelv rendszert érintő jogellenes beavatkozásról szóló 4. Cikke szerint: A tagállamok meghozzák a szükséges intézkedéseket annak érdekében, hogy a valamely információs rendszer működésének számítógépes adatok szándékos és jogosulatlan bevitele, továbbítása, megrongálása, törlése, minőségi rontása, megváltoztatása vagy elrejtése, vagy ilyen adatok szándékos és jogosulatlan hozzáférhetetlenné tétele révén történő *súlyos akadályozása vagy megszakítása*, legalább a súlyosabb esetekben bűncselekménynek minősüljön.

[25] Büntetőjog II. Különös Rész (szerk.: Belovics Ervin), HVG-ORAC Lap- és Könyvkiadó, 2021., 1008. o.

[26] A Szekszárdi Járásbíróság 15.Bpk.392/2021/3. számú büntetővégzése.

iii. A gépjármű lopás és az információs rendszer akadályozással történő megsértésének relációja szempontjából irányadó a Kúria Bfv.962/2021/6. számú ítélete, mely rögzíti, hogy a jármű indításgátló rendszerének arra alkalmas elektronikus eszköz felhasználásával történő hatástalanítása az eltulajdonítás megakadályozását hivatott biztonsági rendszernek a kiiktatását, az eltulajdonítás megakadályozására történő alkalmatlanná tételét jelenti. Amennyiben erre a jármű eltulajdonítást célzó elvétele érdekében kerül sor, úgy halmazat megállapítása nem lehetséges, a cselekmény dolog elleni erőszakkal elkövetett lopás bűntetteként értékelendő, lévén az elkövető ily módon a dolog eltulajdonításának megakadályozására szolgáló eszközt a dolog eltulajdonításának megakadályozására alkalmatlanná teszi.

iv. Az akadályozás elkövetési magatartás tipikus példája továbbá az ún. túlterheléses támadás, ennek kapcsán az utóbbi időben számos híradás jelent meg magyar weboldalakat ért támadások kapcsán, emellett többször lehetett olvasni a konzultációs célból létrehozott egyes oldalak sérülékenységét bemutató, közösségi médiába feltöltött videókkal szemléltetett cselekményekről is. Az egyik ilyen ügyben[27] az elkövető több órányi felvételen dokumentálta, amint az általa készített program véletlenszerűen generált nevekkel és válaszokkal tölti ki a nemzeti konzultációs ívet az erre létrehozott online platformon. Az ügyben megállapítható volt, hogy az elkövető által készített bővítmény az űrlap beküldésével minden egyes alkalommal egységnyi adatmennyiséget küldött az azt feldolgozó szervernek, az adatküldéseket az adott intenzitás mellett a szolgáltató által működtetett DDoS védelmi eszköz nem érzékelte támadásként. A beszerzett adatok alapján megállapítható volt az is, hogy az elkövető által beküldött automatizált kérdőívek mennyisége a teljes kérdőív mennyiség egyharmada volt, azonban a naplófájlok elemzése alapján az elkövető viszonylag ritkán és kis mennyiségű adatot küldött a webszerver felé, melynek következtében a rendszer nem állt le, a cselekmény nagymértékű lassulást sem eredményezett, a rendszer használatát nem akadályozta. Ezen körülményt az elkövetőnek magának is észlelnie kellett, azonban az adatküldések intenzitását jelentősen nem növelte, sőt, adott napokon az éppen csökkent, magát a folyamatot – mely esetlegesen a rendszer akadályozásához vezethetett volna – újra és újra ő maga szakította meg. Csekély időközönként kis mennyiségű adat küldése a webszerver felé önmagában is kizárja annak a lehetőségét, hogy a „tömeges kitöltést" túlterheléses támadásként (vagy annak kísérleteként) lehessen értékelni, mivel ilyen jellegű adatküldés az adott oldal működésének megzavarására egyáltalán nem alkalmas, egy olyan magatartás pedig, amely a konkrét körülmények között semmilyen veszélyt nem jelent a büntetőjog által oltalmazott értékre vagy érdekre, az büntetőjog-ellenes sem lehet[28], így az bűncselekménynek nem tekinthető. Figyelemmel arra, hogy az elkövető cselekménye az információs rendszer megbízható és biztonságos működéséhez fűződő érdeket nem sértette és nem is veszélyeztette, így bűncselekményként nem is volt értékelhető.

v. A Btk. 267. §-ában szabályozott nemzeti adatvagyon körébe tartozó állami nyilvántartás elleni bűncselekménytől[29] való elhatárolás kapcsán szükséges megjegyezni, ha a nyilvántartást

[27] A Fővárosi Főügyészségen G.4794/2020. számon iktatott bűnügy.
[28] Belovics Ervin: Büntetőjog I., HVG-ORAC Lap-és Könyvkiadó Kft., 2017., 324. o.
[29] A Btk. 267. § (1) bekezdése szerint a) a nemzeti adatvagyon körébe tartozó állami nyilvántartásban kezelt adatot az adatkezelő részére hozzáférhetetlenné teszi, vagy b) a nemzeti adatvagyon körébe tartozó állami nyilvántartás működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza, ha súlyosabb bűncselekmény nem valósul meg, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő. Súlyosabban minősül a cselekmény, ha jelentős érdeksérelmet okoz, haszonszerzés végett követik el, vagy ha a bűncselekmény következtében a nemzeti adatvagyon körébe tartozó állami nyilvántartásban kezelt valamennyi adat az adatkezelő részére tartósan hozzáférhetetlenné válik.

elektronikusan, védett számítástechnikai rendszerben vezetik, és az elkövető a nyilvántartást túlterheléses támadással vagy más jellegű hackertámadással hozzáférhetetlenné teszi vagy akadályozza, úgy cselekménye a Btk. 423. §-a szerinti információs rendszer vagy adat megsértése bűncselekményként fog minősülni.[30]

3. Az információs rendszer vagy adat megsértésének Btk. 423. § (2) bekezdésének b) pontjában szabályozott *harmadik alapesetét* követi el, aki információs rendszerben lévő adatot jogosulatlanul vagy jogosultsága kereteit megsértve megváltoztat, töröl vagy hozzáférhetetlenné tesz.

i. A III/1/ii. pontban hivatkozott jogesetben az elkövető az általa üzemeltetett eszközöket a szolgáltató telephelyén kialakított internet végponthoz csatlakoztatta és a gépek működéséhez szükséges adatforgalmat ezeken az eszközökön keresztül biztosította. Ezen végpontok elsődleges célja a rendszer terhelésének monitorozása volt. Minderre tekintettel megállapítható, hogy a csatlakoztatott eszközök okán a szolgáltató rendszere kismértékben a valóságtól eltérő adatokat rögzített. Mindezek alapján az ügyben a Btk. 423. § (2) bekezdés b) pontjába ütköző információs rendszer vagy adat megsértésének bűntette megváltoztatás elkövetési magatartással való elkövetését is vizsgálni volt szükséges. Az információs rendszer vagy adat megsértésének bűntette bűncselekmény ezen fordulatának elkövetési tárgya az információs rendszerben már meglévő adat[31], elkövetési magatartása – egyebek mellett – az adat eredeti információtartalmának elkövető általi jogosulatlan megváltoztatása, vagyis az adat tartalmának bármilyen módon történő módosítása, így felülírása, kiegészítése vagy részleges törlése. Az ügyben az volt megállapítható, hogy a szolgáltató rendszere – mivel az az elkövető által előfizetés használata nélkül generált adatforgalmat nem dokumentálta – a statisztikai hibahatáron belül értelmezhető eltérésben szükségszerűen a valóságtól eltérő terhelési adatokat rögzített. Arra azonban nem merült fel adat, hogy az elkövető a rendszerben már meglévő adatot megváltoztatott volna, minderre figyelemmel a cselekmény nem alkalmas az információs rendszer vagy adat megsértése bűncselekmény harmadik alapesetének megállapítására sem.[32]

ii. A Kúria már hivatkozott, EBH2009.2033. számú döntésének alapját képező ügyben megállapítható tényállás lényege szerint a főiskola számítástechnikai hálózatának felügyeletét ellátó informatikus a hallgatók vizsgakötelezettségét és vizsgaeredményeit nyilvántartó számítástechnikai rendszerben a vizsgát előírás ellenére nem tett hallgatókkal kapcsolatban ellenszolgáltatás fejében olyan adatokat rögzített, amelyek szerint a hallgatók a meghatározott tantárgyból eredményes vizsgát tettek. A Kúria megállapította, hogy az információs rendszerben tárolt adat megváltoztatását jelenti a ténylegesen le nem tett vizsgára vonatkozó adat eredményesen letettként történő rögzítése, függetlenül attól, hogy az adat megváltoztatását végző személy jogosult volt-e a rendszer használatára, avagy sem. A Kúria ebben az ügyben szintén megállapította, hogy az eltérő jogi tárgy sérelme kapcsán a cselekmény a számítástechnikai rendszer és adatok elleni bűncselekmény mellett közokirat-hamisítás és vesztegetés bűntettének megállapítására is alkalmas.

---

[30] A Büntető Törvénykönyv kommentárja ügyészeknek (szerk: Belovics Ervin, Polt Péter), lezárva: 2021. július 8., Elérhető: HVG-Orac Jogkódex (online)

[31] Büntetőjog II. Különös Rész (szerk. : Belovics Ervin), HVG-ORAC Lap- és Könyvkiadó, 2021., 1009. o.

[32] Mindez egybevág az Irányelv 5. Cikkével, mely szerint a tagállamok meghozzák a szükséges intézkedéseket annak érdekében, hogy a valamely információs rendszer számítógépes adatainak szándékos és jogosulatlan törlése, megrongálása, minőségi rontása, megváltoztatása vagy elrejtése, vagy az ilyen adatok szándékos és jogosulatlan hozzáférhetetlenné tétele legalább a súlyosabb esetekben bűncselekménynek minősüljön.

iii. Orgazdaság vétsége mellett a Btk. 423. § (2) bekezdésének b) pontjába ütköző információs rendszer vagy adat megsértésének bűntettében mondta ki bűnösnek a bíróság azt a számítástechnikai eszközök értékesítésével foglalkozó terheltet, aki a lopásból származó telefont megvette, majd annak adattartalmát a gyári állapotba visszaállítva törölte és a készüléket értékesítette.[33]

iv. Időről időre visszatérő típusügynek tekinthetők a sértettel az érintett informatikai eszközön hagyott szöveges fájlban, az eszköz képernyőjén, e-mailben vagy egyéb módon közölt zsaroló üzenetek nyomán indult eljárások. Ezen ügyeket szükséges annak mentén megkülönböztetni egymástól, hogy ténylegesen sor kerül-e zsarolóvírus ("ransomware") használatára, azaz megfertőzésre kerül-e valamilyen informatikai eszköz, avagy sem.

iv/a. Előbbi ügykörbe napjainkban már inkább a nagyobb entitások, cégek, önkormányzatok, kórházak sérelmére elkövetett cselekmények tartoznak.[34] Ezekben az esetekben ténylegesen megtörténik az érintett által használt informatikai rendszer zsarolóvírussal való megfertőzése, megbénítása, melynek helyreállítását „váltságdíj" megfizetésétől teszik függővé. Ebben az esetben a zsarolással halmazatban megállapítható az információs rendszer vagy adat megsértésének bűncselekménye is. Ilyen volt pl. a magyarországi sértettet is érintő WannaCry zsarolóvírus.[35]

iv/b. Utóbbi ügyekben a tényállás alapját a rendszerint magánszemély sértett részére küldött – immár jellemzően feladóként a címzett saját levelezési címét mutató – e-mail képezi, mely szerint az elkövető a sértett informatikai eszközének operációs rendszerét feltörve arra olyan vírust telepített, mely teljes ellenőrzést és hozzáférést biztosít számára a sértett által használt eszközhöz, arról minden adatot átmásolt a szervereire, amelyek között olyan kompromittáló videó is volt, amin az érintett pornográf felvételt néz. Az elkövető az ilyen jellegű e-maileket tipikusan azzal zárja, hogy amennyiben a sértett nem fizet meg adott határidőn belül a megjelölt – jellemzően – bitcoin címekre egy amerikai dollárban, euróban vagy forintban meghatározott összeget, úgy a róla készült kompromittáló videót valamennyi telefonos, e-mailes és közösségi médiás kontaktjának elküldi, ezzel hírnevét tönkreteszi. Bár első ránézésre az ilyen ügyekben a zsarolással anyagi halmazatban áll a tiltott adatszerzés, illetve az információs rendszer elleni bűncselekmény, a gyakorlatban az eljárások során rövid időn belül megállapítást nyer, hogy erről szó sincs. A hasonló ügyek nyomozásában ilyen szempontból is kiemelt jelentősége van az e-mail fejléc elemzésnek.[36] Azokban az esetekben, amikor a sértett látszólag saját magától kapja a zsaroló e-mailt, jellemzően megállapítható, hogy a feladó e-mail címek módosításra, hamisításra kerültek. Ez az ún. e-mail spoofing, mely lényegét tekintve lehetővé teszi az eredeti feladói e-mail cím bármilyen más címre, így a sértett címére történő módosítását is. Mindebből már következtetni lehet arra, hogy az elkövető ténylegesen nem fertőzte meg, illetve törte fel a sértett eszközét, hanem a látszólag a sértett címével egyező e-mail cím használatára a megtévesztés részeként, a zsarolás eredményes kivitelezése érdekében került sor. Az eszköz feltörésének hiányában viszont nyilvánvalóan nem kerülhet sor tiltott adatszerzés vagy információs rendszer elleni bűncselekmény zsarolással halmazatban történő megállapítására.

---

[33] A Szekszárdi Járásbíróság 15.Bpk.362/2021/3. számú büntetővégzése.

[34] Ennek okairól bővebben lsd.: Halász Viktor: Zsarolóvírusok és a No More Ransom projekt, Belügyi Szemle, 2022/9., Elérhető: https://doi.org/10.38146/BSZ.2022.9.9

[35] https://hvg.hu/tudomany/20170516_wannacry_zsarolovirus_magyar_fertozesek

[36] Ehhez több szolgáltató esetében a levelezőprogramokba épített funkció is rendelkezésre áll, azonban az interneten is számos ingyenes program elérhető e célból, pl. a www.mxtoolbox.com oldalon az Analyze Headers fül alatt.

v. Amennyiben az adat megváltoztatása, törlése vagy hozzáférhetetlenné tétele akadályozza az információs rendszer működését és az elkövető tudata mindezt átfogja, tehát az akadályozás tényére egyenes vagy eshetőleg szándéka kiterjed, úgy cselekménye egységesen a Btk. 423. § (2) bekezdésének a) pontjában szabályozott második alapeset szerint minősül.

vi. Az információs rendszer felhasználásával elkövetett csalás – egyebek mellett – az információs rendszerben lévő adat jogosulatlan vagy jogosultsága kereteit megsértő megváltoztatásával, törlésével vagy hozzáférhetetlenné tételével valósulhat meg, ezáltal az információs rendszer vagy adat megsértésének bűntette az információs rendszer felhasználásával elkövetett csalás bűntettének rendszerinti eszközcselekménye. Ennek következtében e két bűncselekmény halmazata látszólagos, csak az információs rendszer felhasználásával elkövetett csalás bűncselekmény megállapításának van helye.

***

Az információs rendszer vagy adat megsértésének minősített esetei a jelentős számú információs rendszert érintő, jelentős érdeksérelmet okozó, illetve közérdekű üzem ellen történő elkövetés. A törvényi tényállásba frissen beiktatott jelentős érdeksérelem okozása kapcsán rögzítést érdemel, hogy a miniszteri indokolás alapján az magában foglalja az ilyen cselekménnyel okozott vagyoni kárt, továbbá az esetleges nem közvetlenül vagyoni értékként, vagyoni kárként azonosítható káros következményeket is (például jelentős mértékű adatvesztés, elhúzódó üzemzavar stb.).

IV. Információs rendszer védelmét biztosító technikai intézkedés kijátszása

A Btk. 424. § (1) bekezdése által szabályozott információs rendszer védelmét biztosító technikai intézkedés kijátszásának vétségét követi el, aki a 375. §-ban, a 422. § (1) bekezdés d) pontjában vagy a 423. §-ban meghatározott bűncselekmény elkövetése céljából az ehhez szükséges vagy ezt könnyítő a) jelszót vagy számítástechnikai programot készít, átad, hozzáférhetővé tesz, megszerez, vagy forgalomba hoz, illetve b) jelszó vagy számítástechnikai program készítésére vonatkozó gazdasági, műszaki, szervezési ismereteit más rendelkezésére bocsátja.

i. A cselekmény kapcsán érdemes kiemelni, hogy amennyiben a saját célra jelszót vagy számítástechnikai programot készítő elkövető a Btk. 375. §-ában, a 422. § (1) bekezdés d) pontjában vagy a 423. §-ban meghatározott bűncselekmény elkövetését megkezdi, úgy az információs rendszer védelmét biztosító technikai intézkedés kijátszása mint önálló szabályozást nyert előkészületi cselekmény, büntetlen előcselekményként értékelendő.

ii. Rögzítendő, hogy az információs rendszer védelmét biztosító technikai intézkedés kijátszása kifejezetten a tényállásban megjelölt három bűncselekmény vonatkozásában követhető el, így pl. ha valaki gépjármű lopások elkövetése érdekében a védelmi rendszer hatástalanításához szükséges programot tartalmazó eszközt készít, úgy cselekménye tényállási elem hiányában információs rendszer védelmét biztosító technikai intézkedés kijátszása vétségének megállapítására nem alkalmas.

iii. A törvényhely (2) bekezdése büntethetőséget megszüntető okot szabályoz, eszerint nem büntethető az (1) bekezdés a) pontjában meghatározott bűncselekmény elkövetője, ha – mielőtt a bűncselekmény elkövetéséhez szükséges vagy ezt megkönnyítő jelszó vagy számítástechnikai

program készítése a büntetőügyekben eljáró hatóság tudomására jutott volna – tevékenységét a hatóság előtt felfedi, az elkészített dolgot a hatóságnak átadja, és lehetővé teszi a készítésben részt vevő más személy kilétének megállapítását.